

Upper ramification jumps in abelian extensions of exponent p

LAURA CAPUANO AND ILARIA DEL CORSO

Abstract

In this paper we present a classification of the possible upper ramification jumps for an elementary abelian p -extension of a p -adic field. The fundamental step for the proof of the main result is the computation of the ramification filtration for the maximal elementary abelian p -extension of the base field K . This result is a generalization of [DCD07, Lemma 9, p. 286], where the same result is proved under the assumption that K contains a primitive p -th root of unity. Using the class field theory and the explicit relations between the normic group of an extension and its ramification jumps, it is fairly simple to recover necessary and sufficient conditions for the upper ramification jumps of an elementary abelian p -extension of K .

1 Introduction

Let K be a finite extension of \mathbb{Q}_p . By the Hasse-Arf Theorem ([Ser79, p.76]), the upper ramification jumps of a finite abelian extension L/K are rational integers. The problem of determining the upper ramification jumps sequence of an extension, as well as the inverse problem to decide whether a set of integers could be the ramification jumps sequence of an extension with a fixed Galois group, is very difficult in general. However, this problem is completely solved in the case of cyclic extensions: a very neat result, due to Maus [Mau73] in the case where $\zeta_p \notin K$, and to Miki [Mik81] in the case where $\zeta_p \in K$, characterizes the sequence of integers which can be the ramification jumps of a totally ramified cyclic p -extension L/K . In this case, the ramification jumps completely determine the sequence of the ramification groups, since the quotients of the filtration are necessarily cyclic of order p .

In this paper we consider another basic case, namely the case of elementary abelian p -extensions of a p -adic field (some results for biquadratic extensions can be found in [BE02]). In this case, the ramification subgroups sequence depends upon the jumps and the order of the subgroups. In Theorem 12, we characterize the sequences of couples of integers (t, m) , where t denotes an upper jump and m its “size” (see Definition 2), which describes the ramification subgroups sequence of an elementary abelian p -extension of K .

Our main tool is the class field theory and the explicit relation, already used in [Sue84] for cyclic extensions, between the normic group of an extension and its ramification jumps. The fundamental step for the proof of Theorem 12 is the computation of the ramification filtration for the maximal elementary abelian p -extension of the base field K . This result is contained in Theorem 11 and is a generalization of [DCD07, Lemma 9, p. 286], where the same result is proved under the assumption that K contains a primitive p -th root of unity.

In the case of non-abelian extensions, the Hasse-Arf Theorem can fail and the upper ramification jumps can be not integral. However, one can give a classification for the lower ramification jumps. In this setting, very few cases are known. One special case can be found in [BE07] where, to better understand the counterexamples to the conclusion of the Hasse-Arf Theorem and as a

first step towards an explicit description of wildly ramified Galois module structure, Byott and Elder classify the ramification break numbers of totally ramified quaternion extensions of dyadic number fields.

2 Notation and preliminary results

Throughout the paper p will be a fixed prime number. If K is a finite extension of \mathbb{Q}_p , we shall denote by e_K and f_K the ramification index and the inertial degree of K/\mathbb{Q}_p , and by n_K the degree of the extension; hence, we have $n_K = e_K f_K = [K : \mathbb{Q}_p]$.

We shall denote also by \mathcal{O}_K the ring of integers of K , by $\pi = \pi_K$ a uniformizer of K (i.e. a generator of the maximal ideal m_K of \mathcal{O}_K) and by v_K the valuation of K normalized so that $v_K(\pi_K) = 1$. We shall indicate the residue field of K by \overline{K} ; then, $|\overline{K}| = p^{f_K}$.

Let U_K be the group of unity of K , and consider its usual filtration $\{U_K^i\}_{i \geq 1}$ given by $U_K^i = 1 + m_K^i$ for $i \geq 1$.

For a finite extension L/K , we denote by $N_{L/K}$, $\mathcal{D}_{L/K}$ and $\text{Disc}_{L/K}$ the norm, the different and the discriminant of L/K respectively. If L/K is a Galois extension with Galois group G , we consider the filtration of G given by the ramification subgroups: in our context, instead of the more classical lower numbering G_i for the ramification subgroups, it is useful to use the upper numbering, so, for every $\nu \geq 0$, we denote the ramification subgroups by G^ν (see [Ser79, Ch. IV] for the definition and the fundamental properties of the ramification subgroups).

We recall here the following theorem which gives a rule to determine the ramification groups of a quotient (see [Ser79, Lemma 5, p. 75]):

Theorem 1 (Herbrand). *If H is a normal subgroup of G , then, for every $\nu > 0$,*

$$(G/H)^\nu = G^\nu H/H.$$

We are interested in studying the filtration of the G^ν and, more specifically, the values of ν for which these subgroups change. We give the following definition:

Definition 1. We say that s is a lower ramification jump for the extension L/K if $G_s \neq G_u$ for every $s > u$. Similarly, we say that t is an upper ramification jump if $G^t \neq G^u$ for every $u > t$.

The lower jumps of an extension are always integers, whereas in general the upper jumps are not necessarily integers. However, in the case of abelian extensions, we have the following theorem (see [Ser79, p.76]):

Theorem 2 (Hasse-Arf). *If G is an abelian group and if ν is a jump in the filtration G^ν , then ν is an integer.*

As already observed in the introduction, the problem of determining whether a set of integers may be realized as the sequence of upper ramification jumps for an extension L/K can be very difficult in general. The problem is completely solved in the case of cyclic extensions.

A necessary and sufficient condition for given m natural numbers $t^1 < \dots < t^m$ to be upper ramification jumps of a totally ramified cyclic p -extension over K was given by Maus ([Mau73], in two cases, namely when $\zeta_p \notin K$ and when, if r is the maximal integer such that $\zeta_{p^r} \in K$, $v_K(\zeta_{p^r} - 1) \not\equiv 0 \pmod{p}$), and by Miki [Mik81] in the general case. A constructive proof of the existence part of Miki's result was given by Sueyoshi in [Sue84].

The general result of Miki is rather technical to state; we at least recall what can happen in the easier case when $\zeta_p \notin K$:

Theorem 3 (Maus, 1973). *Let $\{t^1 < \dots < t^m\}$ be a finite set of integer numbers and suppose that $\zeta_p \notin K$; then, there exists a totally ramified cyclic extension L/K of degree p^m with upper ramification jumps t^1, \dots, t^m if and only if the following conditions hold:*

- $1 \leq t^1 < \frac{pe_K}{p-1}$ and $(t^1, p) = 1$;
- if $t^i < \frac{e_K}{p-1}$, then $t^{i+1} = pt^i$ or $pt^i < t^{i+1} < \frac{pe_K}{p-1}$ and $(p, t^{i+1}) = 1$;
- if $t^i \geq \frac{e_K}{p-1}$, then $t^{i+1} = t^i + e_K$.

Our aim is to characterize the upper ramification jumps and the ramification subgroups of an elementary abelian p -extension of K . In this case, ramification subgroups are clearly elementary abelian p -groups, so the ramification groups sequence is completely determined by the jumps and the order of the subgroups.

Definition 2. Let L/K be a Galois extension with Galois group G and let $t \geq 1$ be an upper ramification jump. If $|G^t/G^{t+1}| = p^m$, we call m the “size” of the upper jump t .

Given an elementary abelian p -extension, we can associate to the ramification subgroups a sequence of couples of integers (t, m) , where t denotes an upper jump and m its size. We will refer to the couple simply as to the ramification jump.

For convenience of the reader, we quote the class field correspondence theorem in a form which easily follows from Theorem 6.2 and 6.3 of [FV02, Ch. III, p. 154].

Theorem 4 (Class field correspondence). *There is a one-to-one correspondence between the finite abelian extensions of K and the subgroups of finite index of K^\times given by $L \longleftrightarrow N_{L/K}(L^\times)$. This correspondence is an order reversing bijection between the lattice of finite abelian extensions of K (with respect to the intersection $L_1 \cap L_2$ and the compositum $L_1 L_2$) and the lattice of subgroups of finite index in K^\times (with respect to the intersection $N_1 \cap N_2$ and the product $N_1 N_2$). Furthermore, if L/K is the extension associated to the normic subgroup N and G is its Galois group, $K^\times/N \cong G$, hence $|K^\times/N| = [L : K]$.*

There is a strict connection between the ramification groups of an extension L/K and the group $K^\times/N_{L/K}(L^\times)$. In the case of totally ramified extensions of degree p , this is given by the following proposition:

Proposition 5. *Let L/K be a totally ramified extension of degree p and let t be its upper ramification jump. Then*

$$t = \min\{j \in \mathbb{N} \mid U_K^{j+1} \subseteq N_{L/K}(L^\times)\}.$$

Proof. Let t be the upper ramification jump of the extension L/K . Following [Ser79, Ch. IV], we denote by $\varphi_{L/K} : \mathbb{R}^+ \rightarrow \mathbb{R}^+$ the Herbrand function and by $\psi_{L/K}$ its inverse. In this way, $G^\nu =: G_{\psi_{L/K}(\nu)}$ for every $\nu > 0$. In our case, an easy calculation gives

$$\psi(n) = \begin{cases} n & \text{if } n \leq t \\ t + p(n - t) & \text{if } n > t \end{cases}$$

From [Ser79, Cor. 1, p. 228], we know that $N_{L/K}(U_L^{\psi(n)}) \subseteq U_K^n$ for every n and the equality holds if and only if $n > t$. It follows that $U_K^{t+1} \subset N_{L/K}(L^\times)$, that is

$$t \geq \min\{j \in \mathbb{N} \mid U_K^{j+1} \subseteq N_{L/K}(L^\times)\}.$$

We have now to show that t is exactly the minimum. If not, we would have $U_K^t \subseteq N_{L/K}(L^\times)$. From [Ser79, Thm 1, p. 227] we know that, for $n \geq 0$, the canonical map induced by inclusion and projection $U_K^n/N_{L/K}(U_L^{\psi(n)}) \longrightarrow K^\times/N_{L/K}(L^\times)$ is injective, hence $U_K^n \cap N_{L/K}(L^\times) = N_{L/K}(U_L^{\psi(n)})$. This means that, if $U_K^n \subseteq N_{L/K}(L^\times)$, we get $U_K^n \subseteq N_{L/K}(U_K^{\psi(n)})$, that is a contradiction if $t = n$. \square

3 The compositum of all extensions of degree p of K

Let $\mathcal{E}_K(p)$ be the set of all the cyclic extensions of K of degree p within a fixed algebraic closure of K and let $\mathcal{C}_K(p)$ be the compositum of all extensions $E \in \mathcal{E}_K(p)$; then, $\mathcal{C}_K(p)$ is the maximal elementary abelian p -extension of K in this fixed algebraic closure. In this section, following [DCD07], we determine the upper ramification jumps of $\mathcal{C}_K(p)/K$.

Proposition 6.

$$[\mathcal{C}_K(p) : K] = \begin{cases} n_K + 1 & \text{if } \zeta_p \notin K \\ n_K + 2 & \text{if } \zeta_p \in K \end{cases}$$

Proof. This is a classical result that can be easily proved using, for example, [Nar90, Ch. V, Prop 5.8 and Thm 5.7]¹. \square

In [DCD07], the ramification subgroups of $\mathcal{C}_K(p)/K$ are computed, using Kummer theory, in the case where $\zeta_p \in K$. The use of the class field theory allows us to generalize this result to a general field K . Also in this general case, the ramification groups can be computed via the study of all the subextensions of degree p .

Let L/K be a Galois extension of degree p and let $\mathcal{D}_{L/K} = \pi_K^{D_L}$. Clearly $L \subseteq \mathcal{C}_K(p)$ and, if $G_L = \text{Gal}(\mathcal{C}_K(p)/L)$, then $\text{Gal}(L/K) \cong G/G_L$.

From the ramification-discriminant formula [Ser79, Prop. 4, p.64], $v_L(\mathcal{D}_{L/K}) = \sum_{i \geq 0} (|G_i| - 1)$. In our case, $|G_i| = p$ if $0 \leq i \leq t$ and 1 otherwise, hence $v_L(\mathcal{D}_{L/K}) = (p-1)(t+1)$ and the jump of this extension is $t = \frac{D_L}{(p-1)} - 1$. Hence,

$$(G/G_L)^\nu = (G/G_L)_\nu = \begin{cases} \mathbb{Z}/p\mathbb{Z} & \text{if } \nu \leq \frac{D_L}{(p-1)} - 1 \\ 0 & \text{if } \nu > \frac{D_L}{(p-1)} - 1 \end{cases}.$$

This information and Herbrand's Theorem 1 allow us to reconstruct the ramification groups of G . In fact, by Herbrand's Theorem, $(G/G_L)^\nu = G^\nu G_L/G_L$, for every $\nu \geq 0$, hence

$$(G/G_L)^\nu = 0 \iff G^\nu \subseteq G_L \iff \nu > \frac{D_L}{(p-1)} - 1.$$

Since G_L runs over all subgroups of index p of G as L runs over all normal extension of degree p of K , it follows that

$$G^\nu = \bigcap_{\substack{L \subseteq \mathcal{C}_K(p) \\ [L : K] = p \\ D_L/(p-1) < \nu + 1}} G_L.$$

This characterization of the ramification subgroups allow us to easily prove the following proposition:

¹This result holds for every complete field with finite residue field.

Proposition 7. *Let M/K be a finite extension with Galois group $(\mathbb{Z}/p\mathbb{Z})^h$; then t is an upper ramification jump of M/K if and only if there exists a subextension L/K of degree p with upper ramification jump equal to t .*

Proof. Assume that there exists a subextension $L \subseteq M$ such that L/K is cyclic of degree p with upper ramification jump t ; we prove that t is an upper ramification jump for M/K .

Let G be the group $\text{Gal}(M/K)$ and $G_L = \text{Gal}(M/L)$; then, $\text{Gal}(L/K) \cong G/G_L = (G/G_L)^t$ and $(G/G_L)^{t+1} = \{1\}$.

By Herbrand's Theorem 1, we have that, for every $s \geq 0$,

$$(G/G_L)^s \cong G^s G_L / G_L \cong G^s / (G^s \cap G_L),$$

hence $(G/G_L)^s = \{1\}$ if and only if $G^s \subseteq G_L$. This proves that $G^{t+1} \subseteq G_L$, whereas $G^t \not\subseteq G_L$, hence t is an upper ramification jump for M/K .

Assume now that t is an upper ramification jump for M/K . From the previous description, we get

$$G^t = \bigcap_{\substack{L \subseteq M \\ [L:K]=p \\ \frac{D_L}{(p-1)} < t+1}} G_L \quad \text{and} \quad G^{t+1} = \bigcap_{\substack{L \subseteq M \\ [L:K]=p \\ \frac{D_L}{(p-1)} < t+2}} G_L.$$

Since $G^t \neq G^{t+1}$, there exists $L \subset M$ with $[L:M] = p$ and $D_L = (p-1)(t+1)$ and the upper ramification jump of this extension is exactly t . \square

We want now to construct a normic group in K^\times such that the corresponding extension is a subextension of $\mathcal{C}_K(p)$ and its Galois group over K has a given jump. To this aim, we need to describe the structure of the unit group U_K .

Let $I = \{i \in \mathbb{Z} \mid 1 \leq i < \frac{pe_K}{p-1} \text{ and } (p, i) = 1\}$, let \overline{K} be the residue field and let us fix a set $C = \{c_1, \dots, c_{f_K}\}$ of elements of \mathcal{O}_K such that the residues of its elements in \overline{K} form a basis of \overline{K} over \mathbb{F}_p . If $\zeta_p \in K$, denote by r the maximal integer such that K contains a p^r -root of unity.

Theorem 8 (Fesenko-Vostokov, Ch. I, Prop. 6.4, p. 19). *Every $\alpha \in U_K^1$ can be written as a convergent product*

$$\alpha = \prod_{i \in I} \prod_{j=1}^{f_K} (1 + c_j \pi^i)^{a_{ij}} \omega_*^a,$$

where:

- if $\zeta_p \notin K$, $\omega_* = 1$, $a = 0$ and the above expression for α is unique, hence U_K^1 is a free \mathbb{Z}_p -module of rank $n = e_K f_K = [K : \mathbb{Q}_p]$;
- if $\zeta_p \in K$, then $\omega_* = 1 + c_* \pi^{\frac{pe_K}{p-1}}$ is a principal unit such that $\omega_* \notin K^p$, $c_* \in C$ and $a \in \mathbb{Z}_p$. In this case, the above expression is not unique, and U_K^1 is a product of a free \mathbb{Z}_p -module of rank n and the p -torsion group μ_{p^r} .

Let us call $F = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid x \in I, 1 \leq y \leq f_K\}$; we put $\eta_{(x,y)} = 1 + c_y \pi^x$ for every $(x, y) \in F$.

It is known that the maximal unramified extension K_{ur} of $\mathcal{C}_K(p)$ is cyclic of degree p (and it is the one associated to the group $\langle K^{\times p}, U_K^1 \rangle$). The following lemma characterizes the maximal subextensions of $\mathcal{C}_K(p)$ with only one ramification jump:

Lemma 9. *Let $t \in I$ and let L_t/K the extension associated to the normic group*

$$N_t = \langle K^{\times p}, \pi, \{\eta_{(x,y)}\}_{(x,y) \in F, x \neq t}, \omega_* \rangle.$$

Then, L_t/K is an elementary abelian extension of degree p^{f_K} with only one ramification jump equal to t .

Proof. By Theorem 4, we have $[L_t : K] = |K^\times/N_t|$. Now, $K^\times/N_t \cong U_K^t/U_K^{t+1}$ and, since $t \in I$, by Theorem 8 we have that $U_K^t/U_K^{t+1} \cong \overline{K}$. It follows that $[L_t : K] = |\overline{K}| = p^{f_K}$. Moreover, since $\langle K^{\times p}, \pi \rangle \subset N_t$, then L_t/K is totally ramified.

Using the previous proposition, it is easy to see that t is a ramification jump for L_t . In fact, we can consider the extension L/K associated to the normic group

$$N = \langle K^{\times p}, \pi, \{\eta_{(x,y)}\}_{(x,y) \in F - \{(t,1)\}}, \omega_* \rangle;$$

L is a subextension of L_t/K since $N_t \subset N$, has degree p (because $|K^\times/N| = p$) and ramification jump equal to t (this follows easily from Proposition 5). By Proposition 7, we have that t is also an upper ramification jump for L_t/K .

We want to show that t is the only possible jump. In fact, let L be any subextension of L_t/K of degree p over K ; then, the group $N_L = N_{L/K}(L^\times)$ is a subgroup of K^\times of index p and contains N_t , so $U_K^{t+1} \subset N_t \subset N_L$.

On the other hand, $K^\times = \langle U_K^t, N_t \rangle$ and $N_L \not\subset K^\times$, so $U_K^t \not\subset N_L$ and, applying Proposition 5, its ramification jump is t . Using Proposition 7, we get that t is the only ramification jump of L_t/K . □

If $\zeta_p \in K$, the field $\mathcal{C}_K(p)$ has also a totally ramified subextension with jump not in the set I :

Lemma 10. *If $\zeta_p \in K$, let $t' = \frac{pe_K}{p-1}$ and let $L_{t'}$ be the extension associated to the normic subgroup*

$$N_{t'} = \langle K^{\times p}, \pi, \{\eta_{(x,y)}\}_{(x,y) \in F} \rangle.$$

Then, $L_{t'}/K$ is a cyclic extension of degree p with ramification jump equal to t' .²

Proof. The argument of the proof is the same in the previous lemma. By the class field theory (Theorem 4), we have that $[L_{t'} : K] = |K^\times/N_{t'}|$ and $|K^\times/N_{t'}|$ is a cyclic group generated by $\omega_* N_{t'}$ that has order p (recall that ω_* is, by Theorem 8, a principal unit of $U_K^{\frac{pe_K}{p-1}}$ such that $\omega_* \notin K^p$). The fact that the ramification jump is exactly t' follows easily from Proposition 5, since $U_K^{t'} \not\subset N_{t'}$ (by construction $\omega_* \notin N_{t'}$) and $U_K^{t'+1} \subseteq K^{\times p} \subseteq N_{t'}$. □

Theorem 11. *If $\zeta_p \notin K$, the upper ramification groups of $\mathcal{C}_K(p)/K$ are the following:*

1. $G = G^{-1} = (\mathbb{Z}/p\mathbb{Z})^{n_K+1}$;
2. $G^0 = \dots = G^{t^1} = (\mathbb{Z}/p\mathbb{Z})^{n_K}$;
3. $G^{t^i+1} = \dots = G^{t^{i+1}} = (\mathbb{Z}/p\mathbb{Z})^{n_K - i f_K}$ for every $i = 1, \dots, e_K - 1$;
4. $G^{t^{e_K}+1} = \{e\}$;

so, the upper ramification jumps are exactly -1 of size 1 and $t^1 \dots t^{e_K}$ of size f_K .

If $\zeta_p \in K$, the upper ramification groups of $\mathcal{C}_K(p)/K$ are the following:

²We recall that, if $\zeta_p \in K$, $(p-1) \mid e_K$ so $\frac{pe_K}{p-1}$ is an integer.

1. $G = G^{-1} = (\mathbb{Z}/p\mathbb{Z})^{n_K+2}$;
2. $G^0 = \dots = G^{t^1} = (\mathbb{Z}/p\mathbb{Z})^{n_K+1}$;
3. $G^{t^i+1} = \dots = G^{t^{i+1}} = (\mathbb{Z}/p\mathbb{Z})^{n_K+1-if_K}$ for every $i = 1, \dots, e_K - 1$;
4. $G^{t^{e_K}+1} = G^{\frac{pe_K}{p-1}} = \{\mathbb{Z}/p\mathbb{Z}\}$;
5. $G^{\frac{pe_K}{p-1}+1} = \{e\}$;

so, the upper ramification jumps are exactly -1 and $\frac{pe_K}{p-1}$ of size 1 and $t^1 \dots t^{e_K}$ of size f_K .

Proof. Let us consider the case $\zeta_p \in K$ (the case $\zeta_p \notin K$ is the same without taking into account the “special subextension” $L_{t'}$). As done before, call $t' = \frac{pe_K}{p-1}$ and $I' = I \cup \{t'\}$. Firstly, we show that $\mathcal{C}_K(p) = K_{ur} L_{t'} \prod_{t \in I} L_t$. In fact, each extension on the right-hand side is an elementary abelian p -extension, so $\mathcal{C}_K(p) \supseteq K_{ur} \prod_{t \in I'} L_t$. On the other hand, K_{ur} is linearly disjoint from $\prod_{t \in I'} L_t$: in fact, for the class field theory and the previous constructions, the extension K_{ur}/K is associated to the normic subgroup $\langle K^{\times p}, U_K^1 \rangle$, while $\prod_{t \in I'} L_t/K$ is associated to the normic subgroup $\cap_{t \in I'} N_t = \langle K^{\times p}, \pi \rangle$. Hence, the intersection of these extensions is the field associated to the normic group $\langle K^{\times p}, \pi, U_K^1 \rangle = K^\times$, namely K .

With the same argument, one can show that, for every $\bar{t} \in I'$, the extension $L_{\bar{t}}$ is linearly disjoint from $\prod_{t \in I' \setminus \{\bar{t}\}} L_t$. It follows that

$$[K_{ur} \prod_{t \in I'} L_t : K] = [K_{ur} : K] \prod_{t \in I'} [L_t : K] = p^{n_K+2} = [\mathcal{C}_K(p) : K],$$

so $\mathcal{C}_K(p) = K_{ur} \prod_{t \in I'} L_t$.

It is clear that all the integers $\{-1, t^1, \dots, t^{e_K}, t'\}$ are upper ramification jumps for the extension $\mathcal{C}_K(p)/K$, as all of them are upper ramification jumps for a cyclic subextension of $\mathcal{C}_K(p)/K$ of degree p (see the proofs of Lemma 9 and 10).

To see that these are the only upper jumps, it is enough to prove that each of the jumps in $\{t^1, \dots, t^{e_K}\}$ has at least size p^{f_K} and t' has size at least one. In this case, in fact, we get:

$$|G/G^0| |G^{t'}/G^{t'+1}| \prod_{t \in I} |G^t/G^{t+1}| \geq p^{2+f_K e_K} = |G|,$$

and this yields $|G^t/G^{t+1}| = p^{f_K}$ for every $t \in I$, $|G^{t'}/G^{t'+1}| = p$ and no more jump is possible.

We already know that $|G/G^0| = p$. Let $t \in I$ and call $H = \text{Gal}(\mathcal{C}_K(p)/L_t)$; by Galois correspondence, $G/H \cong \text{Gal}(L_t/K)$. From the previous lemma, we know that L_t/K has only one upper ramification jump equal to t , so $(G/H)^t = (\mathbb{Z}/p\mathbb{Z})^{f_K}$ and $(G/H)^{t+1} = \{e\}$. On the other hand, Herbrand's Theorem 1 ensures that, for each $s > 0$, we have $(G/H)^s \cong G^s H/H$; moreover, $G^s H/H \cong G^s/G^s \cap H$, so we get $G^{t+1} \subseteq H$, and

$$|G^t/G^{t+1}| = |G^t/G^t \cap H| \cdot |G^t \cap H/G^{t+1}| = |(G/H)^t| \cdot |G^t \cap H/G^{t+1}| \geq p^{f_K},$$

as wanted. The same argument holds if we take $t' = \frac{pe_K}{p-1}$ and the extension $L_{t'}$ constructed in Lemma 10. \square

4 The General Result

The following theorem classifies the sequence of couples of integers which can be the upper ramification jumps of an elementary abelian p -extension of K .

Theorem 12. *Let K be a finite extension of \mathbb{Q}_p . Let $(t^1, m_1) \dots (t^h, m_h)$ be couples of integers with $t^1 < \dots < t^h$; there exists an elementary abelian p -extension M/K with upper ramification jumps $(t^1, m_1) \dots (t^h, m_h)$ if and only if the following conditions hold:*

1. *for every $i = 1, \dots, h$, it holds $1 \leq t^i < pe_K/(p-1)$ and $(t^i, p) = 1$ with only two possible exceptions, namely $t^1 = -1$ and, in the case when $\zeta_p \in K$, $t^h = \frac{pe_K}{p-1}$;*
2. *$1 \leq m_i \leq f_K$ for every $i = 1, \dots, h$, $m_1 = 1$ if $t^1 = -1$ and $m_h = 1$ if $t^h = \frac{pe_K}{p-1}$.*

In this case, $[M : K] = \sum_{i=1}^h m_i$.

Proof. Let M be a subextension of $\mathcal{C}_K(p)/K$ and let $(t^1, m_1) \dots (t^h, m_h)$ be its ramification jumps. From Proposition 7, we know that the jumps of M/K are among those of $\mathcal{C}_K(p)/K$, hence t^1, \dots, t^h verify condition (1). Moreover, denoting by H the subgroup of $G = \text{Gal}(\mathcal{C}_K(p)/K)$ fixing M , we have that the ramification filtration of M/K is $(G/H)^{t^i}$ and $|(G/H)^{t^i}/(G/H)^{t^i+1}| = p^{m_i}$. Arguing as in the proof of Theorem 11, we have

$$\left| \frac{(G/H)^{t^i}}{(G/H)^{t^i+1}} \right| = \left| \frac{G^{t^i}/G^{t^i+1}}{G^{t^i} \cap H/G^{t^i+1} \cap H} \right| = p^{f_K} / |G^{t^i} \cap H/G^{t^i+1} \cap H|,$$

hence $1 \leq m_i \leq f_K$ if $t^i \in I$ and $m_1 = 1$ if $t^1 = -1$. Moreover, if $\zeta_p \in K$ and $t^h = \frac{pe_K}{p-1}$, then $|G^{t^h}/G^{t^h+1}| = p$ as seen before, so $m_h = 1$, namely, the m_i verify condition (2).

On the other hand, let $(t^1, m_1), \dots, (t^h, m_h)$ be a sequence verifying conditions (1) and (2); we construct an extension M/K with these ramification jumps.

For each $i = 1, \dots, h$ let M_i/K be any subextension of degree p^{m_i} of L_{t^i}/K , where L_{t^i} is the extension defined in Lemma 9 when $t^i \in I$, $L_{t^h} = L_{t'}$ (the extension defined in Lemma 10) if $t^h = \frac{pe_K}{p-1}$ and $L_{t^1} = K_{ur}$ if $t^1 = -1$. Put $M = \prod_{i=1}^h M_i$; then, using the same techniques applied in Theorem 11, it is easy to see that the ramification jumps of M/K are exactly $(t^1, m_1), \dots, (t^h, m_h)$. \square

Remark 13. If $\zeta_p \in K$, we can prove the same results using another approach, namely using Kummer theory (see [CF67, p. 89]). This method is more explicit as, in this way, we can construct an extension with fixed ramification jumps giving explicit generators.

In fact, by Kummer theory, we know that every p -extension is Galois and of the form $L = K(\sqrt[p]{a})$, with $a \in K^\times / K^{\times p}$. In particular, the element a allows to determine the ramification jump of the extension L/K . More precisely, the following proposition holds:

Proposition 14. *Let us take $a \in K^\times / K^{\times p}$ and let us consider the extension $L = K(\sqrt[p]{a})$. Call t the ramification jump; then:*

- *if $0 < v_K(a) < p$, then $t = \frac{pe_K}{p-1}$;*
- *if $v_K(a) = 0$ and $v_K(a-1) = l$ with $1 \leq l < \frac{pe_K}{p-1}$ and $(l, p) = 1$, then $t = \frac{pe_K}{p-1} - l$;*
- *if $v_K(a) = 0$ and $v_K(a-1) = \frac{pe_K}{p-1}$, then $t = -1$ (and the extension is unramified).*

Proof. If $0 < v_K(a) < p$ and z is a p -th root of a , we can notice that, for every h such that $(h, p) = 1$, $K(z) = K(z^h)$, hence we can restrict to the case $v_K(a) = 1$.

If g is a generator of $\text{Gal}(L/K)$, we have $v_K(g(\pi) - \pi) = v_L(z\pi - \pi) = v_L(z - 1) + v_L(\pi) = \frac{pe_K}{p-1} + 1$, hence $t = \frac{pe_K}{p-1}$.

If $a \in U_K^l \setminus U_K^{l+1}$, from the proof of [DCD07, Lemma 6, p. 15] we have that $v_L(\mathcal{D}_{L/K}) = (\frac{pe_K}{p-1} - l + 1)(p - 1)$. On the other hand, from the ramification-discriminant formula used in Section 3, $v_L(\mathcal{D}_{L/K}) = (p - 1)(t + 1)$. Comparing this with the previous expression, we have $t = \frac{pe_K}{p-1} - l$. Finally, if $a \in U_K^{\frac{pe_K}{p-1}}$, using Hensel's Lemma [CF67, p. 84], it is easy to see that the extension L/K is unramified, hence the ramification jump is $t = -1$. \square

With this relation between the upper ramification jump and the valuation of the generator, one can easily give generators for the subextensions $L_t \subset \mathcal{C}_K(p)$ constructed in Lemma 9. Hence, the following proposition holds:

Proposition 15. Take $t \in I$ and call $l = \frac{pe_K}{p-1} - t$; the extension $L_t = K(\sqrt[p]{\eta_{(x,l)}}, x = 1, \dots, f_K)$ is an elementary abelian extension of degree p^{f_K} over K with just one ramification jump equal to t .

If $t = \frac{pe_K}{p-1}$, the extension $L_t = K(\sqrt[p]{\pi})$ is a totally ramified extension of degree p with ramification jump equal to $\frac{pe_K}{p-1}$.

If $t = -1$, the extension $L_{-1} = K(\sqrt[p]{\omega_*})$ is the only unramified extension of K of degree p and has ramification jump equal to -1 .

LAURA CAPUANO
Scuola Normale Superiore
Piazza dei Cavalieri, 7
56127 Pisa (ITALY)
E-mail: laura.capuano@sns.it

ILARIA DEL CORSO
Dipartimento di Matematica
Largo Bruno Pontecorvo, 5
56127 Pisa (ITALY)
E-mail: delcorso@dm.unipi.it

References

- [BE02] N.B. Byott and G.G. Elder, *Byquadratic Extensions with One Break*, Canad. Math. Bull. **2** (2002), 168–179.
- [BE07] ———, *On wild ramification in quaternion extensions*, J. Théor. Nombres de Bordeaux (2007), 101–124.
- [CF67] J.W.S. Cassels and A. Fröhlich, *Algebraic Number Theory*, Academic Press, 1967.
- [DCD07] I. Del Corso and R. Dvornicich, *The compositum of wild extensions of local fields of prime degree*, Monatsh. Math. **150** (2007), 271–288.
- [FV02] I.B. Fesenko and S.V. Vostokov, *Local Fields and Their Extensions*, 2nd Edition, American Mathematical Society, 2002.
- [Mau73] E. Maus, *Relationen in Verzweigungsgruppen*, J. Reine Angew Math. **258** (1973), 23–50.
- [Mik81] H. Miki, *On the ramification numbers of cyclic p -extensions over local fields*, J. Reine Angew Math. **328** (1981), 99–115.
- [Nar90] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, 2nd Edition, Springer-Verlag, 1990.
- [Ser79] J.P. Serre, *Local Fields*, Springer-Verlag, 1979.
- [Sue84] Y. Sueyoshi, *On ramification of p -extensions of p -adic number fields*, Mem. Fac. Sci., Kyushu University Sez. A **32** (1984), no. 2, 199–204.